



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/519,774	12/22/2004	Christopher Newell Toomey	AOL.022A	7314

20995 7590 11/26/2008  
KNOBBE MARTENS OLSON & BEAR LLP  
2040 MAIN STREET  
FOURTEENTH FLOOR  
IRVINE, CA 92614

EXAMINER
----------

TRUVAN, LEYNNA THANH

ART UNIT	PAPER NUMBER
----------	--------------

2435

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

11/26/2008

ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

jcartee@kmob.com  
eOAPilot@kmob.com



**DETAILED ACTION**

1. Claims 1-5 and 10-20 are pending.  
Claims 6-9 are cancelled by applicant.  
Claims 13-20 are new.

***Response to Arguments***

2. Applicant's arguments with respect to claims 1-5 have been considered but are moot in view of the new ground(s) of rejection.

Claims 1-5 are now rejected under *35 U.S.C. 103(a)* in view of Sandhu and Hinton combination.

3. Applicant's arguments filed 8/1/2008 have been fully considered but they are not persuasive.

Sandhu remains the primary reference for the rejection of 10-12. Claims 1-5 and 10-20 are now rejected under *35 U.S.C. 103(a)* in view of Sandhu and Hinton combination.

Sandhu teaches and suggests stored information about partner sites that have been linked by a user since there involves a cookie with information that corresponds back to the user. Sandhu's information includes password or key and IP address (col.7, lines 33-45), IP number (col.8, lines 63-67), names, roles, and credit card numbers (col.9, lines 40-67). These are variety of information that links to the user for the server to verify during validation/authentication process. Thus, Sandhu reads on the claimed invention. Hinton is combined with Sandhu to disclose the claimed login ticket that it would have been obvious for a person of ordinary skills in the art at the time the invention was made to teach login ticket of Hinton to the apparatus and method of Sandhu because simplifies

Art Unit: 2435

single sign-on capabilities that need not re-authenticate the user and would enhance the usability of the e-community with multiple participating domains (Hinton-col.2, lines 56-67 and col.10, lines 21-54).

As for independent claim 10, the response above applies to claim 10. All dependent claims are also rejected by virtue of the pendency.

***Claim Rejections - 35 USC § 103***

*The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:*

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

**4. Claims 1-5 and 10-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sandhu, et al. (US 6,985,953) in view of Hinton, et al. (US 6,993,596).**

***As per claim 1:***

Sandhu, et al. discloses a apparatus for a baseline authentication agency for determining a user's login status as the user accesses a site within a network, said apparatus comprising:

a database storing information about partner sites that have been linked by a user;

**(col.12, lines 25-30 and col.14, lines 4-6)**

a baseline authentication agencies responsible for core global network authentication services configured: (col.6, lines 38-45; authentication agencies can broadly be given in light of servers, web site, providers, domains, or etc. that provides services.)

to receive a request from a user's browser, the request comprising: a site identification identifying a site; and (col.2, lines 20-31 and col.5, lines 2-31 and 50-60)

a cookie related to the user and including a reference to the baseline authentication agency; (col.8, lines 1-47 and col.10, lines 1-28)

to determine whether the cookie is valid; (col.2, lines 4-17 and col.10, lines 8-14)

to determine whether the user has authorized seamless login for the site using the information from the database; and (col.6, lines 38-45 and col.7, lines 51-67)

to generate a login ticket for the site and send the login ticket to the user's browser if the cookie is valid and the user has authorized seamless login for the site; (col.4, lines 25-67 and col.3, lines 1-12)

wherein the cookie is stored on a global network domain used for cookie sharing and the site is one of (col.5, lines 20-31 and col.14, lines 4-6) a collection of partner sites with access to cookies shared on the global network domain. (col.2, lines 4-20 and col.5, lines 2-16; partner site can broadly be given in light of an affiliated domain/site and server as the authentication agency)

Although, Sandhu discloses login process and authentication agencies but did not include login ticket.

Hinton discloses the invention of allowing an Internet user to transfer directly to a domain that is participating in the e-community without returning to a home domain prior

to transferring to the participating domain. This enhances the usability of the e-community and set of participating domains, and allows the use to build long-term relationship with multiple participating domains (col.2, lines 56-67). Hinton discloses an introductory authentication token which is also referred as a vouch for token and includes the e-community single-sign-on functionality (col.3, lines 49-65 and col.14, line 52-col.15, line 67). Thus, suggests the claimed network global user having a global network account logging onto a global network partner site without preexisting authentication (col.10, line 47-col.13, line 36). Hinton includes an identity cookie DIDC and an enrollment token (or ticket) for the user that can be sent in clear or cryptographically protected (col.7, lines 32-61). Hinton further discusses the e-community cookie indicates the security server or other plug-in location, and a URI at a plug-in location that can provide an authentication vouch for token for that user (col.10, lines 21-46). This allows for simplified single sign-on capabilities within a domain that is partitioned by multiple server domains and that the e-community cookie indicates that the server need not re-authenticate the user (col.10, line 47-col.11, line 42).

Therefore, it would have been obvious for a person of ordinary skills in the art at the time the invention was made to teach login ticket of Hinton to the apparatus and method of Sandhu because simplifies single sign-on capabilities that need not re-authenticate the user and would enhance the usability of the e-community with multiple participating domains (Hinton-col.2, lines 56-67 and col.10, lines 21-54).

As per claim 2: see col.5, lines 20-67 and col.9, lines 11-67; discussing the apparatus of claim 1, wherein the baseline authentication agency provides authentication services for a

Art Unit: 2435

subset of users of the global network domain, the baseline authentication agency server further configured to:

after authenticating the user, write the site identification along with an authenticated status of true into the cookie of the user stored on the global network domain and shared accessible by the collection of partner sites; and after the user logs out of said global network, resets the user's authenticated status to false in said shared domain cookie.

As per claim 3: see col.4, lines 24-67 and col.5, lines 3-31; discussing the apparatus of claim 1, wherein the baseline authentication agency server is configured to: receive the ticket from the site; determine whether the ticket is valid; and if the ticket is valid, send user identification information to the site, the user identification information to be used by the site to login the user.

As per claim 4: see col.5, lines 45-67 and col.6, lines 1-35; discussing the apparatus of claim 1, wherein the baseline authentication agency server is further configured to: send a message to the user's browser that indicates that no ticket is available if the cookie is not valid or if the user has not authorized seamless login for the site.

As per claim 5: see col.3, lines 23-30 and col.5, lines 20-31; discussing the apparatus of claim 1, wherein the baseline authentication agency server further comprises: a globally unique identifier for each global network user account, wherein said globally unique identifier is a primary key with which the database is indexed.

As per claims 6-9: CANCELLED.

***As per claim 10:***

Sandhu, et al. discloses a computer-implemented method for a baseline authentication agency that determines a user's login permission for a site, the method comprising:

receiving a request from a user's browser, the request comprising a site identifier related to a site, and a set of user information related to a user **(col.2, lines 20-31 and col.5, lines 2-31)** and including a reference designating the baseline authentication agency; **(col.8, lines 1-47 and col.10, lines 1-28)**

determining whether the set of user information is valid; **(col.2, lines 4-17 and col.10, lines 8-14)**

if the set of user information is valid, **(col.10, line 60-col.11, line 7 and lines 50-60)**

determining whether the user has authorized seamless login for the site;  
and **(col.6, lines 38-45 and col.7, lines 51-67)**

generating a [login ticket] for the site **(col.4, lines 25-67 and col.3, lines 1-12)** and sending the [login ticket] to the user's browser if the user has authorized seamless login for the site; **(col.11, lines 1-60 and col.14, lines 4-6)**

Although, Sandhu discloses login process and authentication agencies but did not include login ticket.

Hinton discloses the invention of allowing an Internet user to transfer directly to a domain that is participating in the e-community without returning to a home domain prior to transferring to the participating domain. This enhances the usability of the e-community and set of participating domains, and allows the use to build long-term relationship with



multiple participating domains (col.2, lines 56-67). Hinton discloses an introductory authentication token which is also referred as a vouch for token and includes the e-community single-sign-on functionality (col.3, lines 49-65 and col.14, line 52-col.15, line 67). Thus, suggests the claimed network global user having a global network account logging onto a global network partner site without preexisting authentication (col.10, line 47-col.13, line 36). Hinton includes an identity cookie DIDC and an enrollment token for the user that can be sent in clear or cryptographically protected (col.7, lines 32-61). Hinton further discusses the e-community cookie indicates the security server or other plug-in location, and a URI at a plug-in location that can provide an authentication vouch for token for that user (col.10, lines 21-46). This allows for simplified single sign-on capabilities within a domain that is partitioned by multiple server domains and that the e-community cookie indicates that the server need not re-authenticate the user (col.10, line 47-col.11, line 42).

Therefore, it would have been obvious for a person of ordinary skills in the art at the time the invention was made to teach login ticket of Hinton to the apparatus and method of Sandhu because simplifies single sign-on capabilities that need not re-authenticate the user and would enhance the usability of the e-community with multiple participating domains (Hinton-col.2, lines 56-67 and col.10, lines 21-54).

As per claim 11: see Sandhu on col.10, line 60-col.11, line 7 and Hinton on col.7, lines 2-16 and col.10, lines 21-30; discussing a method of claim 10 further comprising checking if the site identifier is known or valid.

As per claim 12: see Sandhu on col.2, lines 32-44 and Hinton on col.3, lines 4-15;

Art Unit: 2435

discussing a method of claim 10, further comprising generating JavaScript code writing out an HTML form comprising the login ticket as a hidden field and writing out a partner Web site global network login handler as an action URL, and auto-submitting said form such that the browser posts the form to a partner Web site global network login handler URL on the partner site.

As per claim 13: see Sandhu on col.2, lines 32-44 and Hinton on col.3, lines 4-15; discussing a method of Claim 10, wherein the set of user information is a cookie.

As per claim 14: see Sandhu on col.2, lines 32-44 and Hinton on col.3, lines 4-15; discussing a method of Claim 10, wherein the site is one of a collection of partner sites.

As per claim 15: see Sandhu on col.2, lines 32-44 and Hinton on col.3, lines 4-15; discussing a method of Claim 10, wherein generating the Login ticket for the site comprises generating JavaScript code that stores the Login ticket.

As per claim 16: see Sandhu on col.2, lines 32-44 and Hinton on col.3, lines 4-15; discussing a method of Claim 15, wherein sending the Login ticket for the site comprises sending the JavaScript code.

As per claim 17: see Sandhu on col., lines and Hinton on col., lines ; discussing a method of Claim 10, further comprising if the set of user information is valid, receiving the ticket from the site; determining whether the ticket is valid; and if the ticket is valid, sending user identification information to the site, the user identification information to be used by the site to Login the user.

As per claim 18: see Sandhu on col., lines and Hinton on col., lines ; discussing a storage medium having a computer program stored thereon for causing a suitably programmed

system to process computer-program code by performing the method of Claim 10 when such program is executed on the system.

***As per claim 19:***

Sandhu, et al. discloses a baseline authentication agency configured to determine a user's login permission for a site, the baseline authentication agency comprising:

a list of partner sites that have been linked by a user; **(col.12, lines 25-30 and col.14, lines 4-6)**

a baseline authentication agency server configured to:

receive a request from a user's browser, the request comprising a site identifier related to a site **(col.2, lines 20-31 and col.5, lines 2-31 and 50-60)**, and a set of user information related to a user and referencing the baseline authentication agency; **(col.8, lines 1-47 and col.10, lines 1-28)**

determine whether the set of user information is valid; **(col.2, lines 4-17 and col.10, lines 8-14)**

determine whether the user has authorized seamless Login for the site; and **(col.6, lines 38-45 and col.7, lines 51-67)**

if the set of user information is valid and the user has authorized seamless login for the site, generate a login ticket for the site; **(col.4, lines 25-67 and col.3, lines 1-12)**

send the Login ticket to the user's browser. **(col.11, lines 1-60 and col.14, lines 4-6)**

Although, Sandhu discloses login process and authentication agencies but did not include login ticket.

Hinton discloses the invention of allowing an Internet user to transfer directly to a domain that is participating in the e-community without returning to a home domain prior to transferring to the participating domain. This enhances the usability of the e-community and set of participating domains, and allows the use to build long-term relationship with multiple participating domains (col.2, lines 56-67). Hinton discloses an introductory authentication token which is also referred as a vouch for token and includes the e-community single-sign-on functionality (col.3, lines 49-65 and col.14, line 52-col.15, line 67). Thus, suggests the claimed network global user having a global network account logging onto a global network partner site without preexisting authentication (col.10, line 47-col.13, line 36). Hinton includes an identity cookie DIDC and an enrollment token for the user that can be sent in clear or cryptographically protected (col.7, lines 32-61). Hinton further discusses the e-community cookie indicates the security server or other plug-in location, and a URI at a plug-in location that can provide an authentication vouch for token for that user (col.10, lines 21-46). This allows for simplified single sign-on capabilities within a domain that is partitioned by multiple server domains and that the e-community cookie indicates that the server need not re-authenticate the user (col.10, line 47-col.11, line 42).

Therefore, it would have been obvious for a person of ordinary skills in the art at the time the invention was made to teach login ticket of Hinton to the apparatus and method of Sandhu because simplifies single sign-on capabilities that need not re-authenticate the user and would enhance the usability of the e-community with multiple participating domains (Hinton-col.2, lines 56-67 and col.10, lines 21-54).

As per claim 20: see Sandhu on col., lines and Hinton on col., lines ; discussing a baseline authentication agency of Claim 19, wherein the baseline authentication agency server is further configured to: receive the ticket from the site; determine whether the ticket is valid; and if the ticket is valid, send user identification information to the site, the user identification information to be used by the site to login the user.

### ***Conclusion***

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Leynna T. Truvan whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/L. T. T./  
Examiner, Art Unit 2435  
/Kimyen Vu/  
Supervisory Patent Examiner, Art Unit 2435